

#2  
7-23-01  
B. Hilliard

Docket No. 1359.1041/HJS  
**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

11036 U.S. PTO  
09/788474  
02/21/01

In re Application of:

Masatoshi SHIOUCHI et al.

Group Art Unit:

Serial No.:

Examiner:

Filed: February 21, 2001

For: VIRTUAL COMMUNICATION CHANNEL AND VIRTUAL PRIVATE  
COMMUNITY, AND AGENT COLLABORATION SYSTEM AND AGENT  
COLLABORATION METHOD FOR CONTROLLING THE SAME

**SUBMISSION OF CERTIFIED COPY OF PRIOR  
FOREIGN APPLICATION IN ACCORDANCE WITH  
THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Assistant Commissioner for Patents  
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s)  
herewith a certified copy of the following foreign application(s):

Japanese Patent Application No. 2000-272195  
Filed: September 7, 2000

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing  
date, as evidenced by the certified papers attached hereto, in accordance with the requirements  
of 35 U.S.C. § 119.

Respectfully submitted,  
STAAS & HALSEY LLP

Date: February 21, 2001

By: \_\_\_\_\_

H. J. Staas

Registration No. 22,010

700 Eleventh Street, N.W., Suite 500  
Washington, D.C. 20001  
Telephone: (202) 434-1500  
Facsimile: (202) 434-1501

日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

J1036 U.S. PTO  
09/788474  
02/21/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 9月 7日

出 願 番 号

Application Number:

特願2000-272195

出 願 人

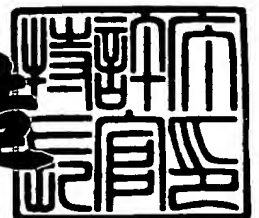
Applicant (s):

富士通株式会社

2001年 1月 5日

特許庁長官  
Commissioner,  
Patent Office

及 川 耕 造



出証番号 出証特2000-3109011

【書類名】 特許願

【整理番号】 0095180

【提出日】 平成12年 9月 7日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 13/00

【発明の名称】 仮想通信路および仮想通信路を制御するエージェント連携システムおよびエージェント連携方法

【請求項の数】 9

【発明者】

    【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

    【氏名】 塩内 正利

【発明者】

    【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

    【氏名】 岩尾 忠重

【発明者】

    【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

    【氏名】 岡田 誠

【発明者】

    【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

    【氏名】 山崎 重一郎

【発明者】

    【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

    【氏名】 毛利 隆夫

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 和田 裕二

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 西ヶ谷 岳

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 福田 茂紀

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100095555

【弁理士】

【氏名又は名称】 池内 寛幸

【電話番号】 06-6361-9334

【手数料の表示】

【予納台帳番号】 012162

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9803089

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 仮想通信路および仮想通信路を制御するエージェント連携システムおよびエージェント連携方法

【特許請求の範囲】

【請求項 1】 エージェント間を仮想通信路により結んだエージェント連携システムであって、前記仮想通信路上の各エージェントが、

エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーを記憶するポリシー記憶部を備え、前記ポリシーに従って各エージェントの属性に応じた権限を付与する権限付与部と、

前記権限付与部により付与された権限および該権限内容が実行される条件を保持・記憶する権限・実行条件保持部と、

前記権限内容の実行条件が成立した場合に該当する権限内容を実行する処理実行部を備え、

前記ポリシーに従って前記仮想通信路を介して各エージェントが連携することを特徴とするエージェント連携システム。

【請求項 2】 前記ポリシーが、エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールに加え、データオブジェクトが持つ属性とエージェントから該データオブジェクトに対する操作に関する反応との関係を表わすルールと、前記権限の集合と前記反応の集合同士の関係を表わすルールと、前記権限の集合間の関係を表わすルールのいずれかまたはすべてを含む請求項 1 に記載のエージェント連携システム。

【請求項 3】 エージェント自らが生成したポリシーを他のエージェントに配布し、

前記配布されたポリシーを受け取った他のエージェントが、該ポリシーに従って前記権限付与部を用いてエージェントの属性に応じた権限を得て前記アクション実行部を構成し、

前記配布されたポリシーを共通に持つエージェント間で仮想通信路を形成する請求項 1 に記載のエージェント連携システム。

【請求項 4】 前記仮想通信路上に認証機構を備え、

前記認証機構が、各エージェントの前記仮想通信路へのアクセス権の認証、各エージェントの権限・実行条件保持部が保持する権限内容の認証を行う請求項 1 に記載のエージェント連携システム。

【請求項 5】 前記認証機構が、ポリシー管理機関と、属性管理機関と、個体認証管理機関の 3 つの機関に分かれ、

前記ポリシー管理機関が、ポリシーを記述したデータに対して電子署名を付し、真正のポリシーであることが認証されたポリシー証明書を発行し、

前記属性管理機関が、各エージェントが持っている属性を証明した属性証明書を発行し、

前記公開鍵管理機関が、ネットワーク上におけるエージェントの個体認証を行った証明である公開鍵証明書を発行し、

各エージェントが、前記ポリシー証明書と属性証明書を解釈するトラストエンジンを備え、ネットワーク上で配布されたポリシー証明書と属性証明書に基づいて前記権限付与部に対して割り当てべき適切な権限内容を指定する請求項 4 に記載のエージェント連携システム。

【請求項 6】 各エージェントが、仮想通信路にログインする際に、前記トラストエンジンを用いて、当該仮想通信路に対応するポリシーの証明書と属性証明書を入力として、ポリシーの証明を得つつログインし、

各エージェントのログインの連鎖により仮想通信路に参加するエージェント間にポリシーを安全に伝播させることを特徴とする請求項 1 に記載のエージェント連携システム。

【請求項 7】 ネットワーク上に存在するエージェント間の情報通信を仲介する方法であって、前記仮想通信路上の各エージェントにおいて、

エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーを記憶し、前記ポリシーに従って各エージェントの属性に応じた権限を付与し、

前記付与された権限および該権限内容が実行される条件を保持・記憶し、

前記権限内容の実行条件が成立した場合に該当する権限内容を実行し、

前記ポリシーに従って前記仮想通信路を介して各エージェントを連携させるこ

とを特徴とするエージェント連携方法。

【請求項 8】 ネットワーク上に存在するエージェント間の情報通信を仲介する処理プログラムを記録したコンピュータ読み取り可能な記憶媒体であって、

エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーを記憶し、前記ポリシーに従って各エージェントの属性に応じた権限を付与する処理ステップと、

前記付与された権限および該権限内容が実行される条件を保持・記憶する処理ステップと、

前記権限内容の実行条件が成立した場合に該当する権限内容を実行する処理ステップと、

各エージェントが前記ポリシーに従って与えられた権限に応じてメッセージをやりとりするように前記仮想通信路を制御する処理ステップとを備えた処理プログラムを記録したことを特徴とする記録媒体。

【請求項 9】 ネットワーク上に存在するエージェント間の情報通信を仲介する通信路であって、

エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーに従って制御され、

前記ポリシーに従って各エージェントに対してその属性に応じた権限を持たせ

、  
前記ポリシーに従って動作するエージェント同士を仮想的に結び、前記権限内容の実行を通して各エージェントの連携処理を仲介することを特徴とする仮想通信路。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、ネットワーク上に存在するエージェントなどコンピュータリソース間においてエージェント連携サービスを提供するエージェント連携装置および方法およびエージェント連携プログラムを格納したコンピュータ読み取り可能な記録媒体に関する。また、必要に応じてエージェント等の間に動的に生成するネッ

トワーク上の仮想的な通信路に関する。

【 0 0 0 2 】

【従来の技術】

近年、コンピュータネットワークが進展し、ネットワーク上に分散した複数のエージェントなどコンピュータリソース間における情報通信サービスが提供されている。従来の技術において、ネットワーク上に存在する複数の通信主体の間を通信路により結ぶ方式として、情報を送信する通信主体が当該情報を受信する通信主体を特定して個別に配信する方式（ピアツーピア接続方式）と、情報を送信する通信主体が当該情報を受信する通信主体を特定することなくネットワーク上に存在する通信主体すべてに対して情報を配信する方式（マルチキャスト方式）がある。

【 0 0 0 3 】

前者のピアツーピア接続方式においても、情報送信において1つの通信主体からメーリングリストなどを用いた同報通信や一斉通信というサービスは可能である。しかし、これは、通信相手のアドレスを指定した1対1の通信が重疊的に行われたものであって、情報送信する通信主体と情報を受信する通信主体との関係でみれば、通信相手を特定して個別に情報を配信するという点において変わらない。

【 0 0 0 4 】

後者の複数の通信主体を接続するマルチキャスト方式としては、CORBA（The Common Object Request Broker : Architecture and Specification）のイベントサービス（Event service）やアイピーマルチキャスト（IP-Multicast）、インターネットリレーチャット（Internet Relay Chat : IRC）などが知られている。これら通信サービスは複数のサーバ間で通信を制御するものである。このように複数のサーバを介したエージェント連携サービスの構築のためには複数のサーバを所定のプロトコルで接続・管理する必要があり、それぞれのサーバの実装は、エージェント連携するサービス内容によってチューニングしなければならない。

【 0 0 0 5 】



イベントサービス (Event service) の特徴としては、通信路への参加に関しては、通信サーバが能動的に目的とする情報がやり取りされている通信ネットワークに対して所定の手順により参加しなければならない。エージェント連携するサービス内容としては、システムのエラー通知が主眼となっており、エラー通知に関するサービスが実装されている。制約としては、メッセージを受信するサーバはデータ受信用のオブジェクトを作成し、特定のトピックに登録しなければならないという制約がある。

#### 【 0 0 0 6 】

アイピーマルチキャスト (IP-Multicast) の特徴としては、通信路への参加に関しては、通信サーバが能動的に目的とする情報がやり取りされている通信ネットワークに対して所定の手順により参加しなければならない。制約としては、マルチキャストする受信相手のアドレスを予め登録しておかなければならないという制約がある。

#### 【 0 0 0 7 】

インターネットリレーチャット (Internet Relay Chat : IRC) の特徴としては、通信路への参加に関しては、通信サーバが能動的に目的とする情報がやり取りされている通信ネットワークに対して所定の手順により参加しなければならない。また、エージェント連携するサービス内容としては、ユーザ同士のテキスト通信が主眼である。制約としては、IRCプロトコルにより通信しなければならないという制約がある。

#### 【 0 0 0 8 】

##### 【発明が解決しようとする課題】

上記従来の技術のピアツーピア接続方式において、メーリングリストなどにより複数のネットワーク上のエージェント等のリソース間の情報通信を行う場合、あらかじめ配信先となる全ての相手のアドレスを登録しておく必要がある。情報配信に際して、情報を配信するエージェント (ユーザ) がすべての配信先を意識的に把握しておく必要が生じることとなる。しかし、情報配信者が必ずしも情報を受信すべき相手を意識的に把握しておくことができない場合もあり、また、多数の配信先を管理することは負担が大きい。広範囲かつ多数の相手に配信するこ

とは非常に困難であり、スケーラビリティに欠けることとなる。さらに、エージェント連携システムが介在するわけではないので、配信の成否についても配信側のエージェントが責任を持つ必要がある。このため、個々のエージェントの負担が非常に大きくなってしまうという問題がある。

## 【 0 0 0 9 】

上記従来の技術の複数の通信主体を接続するマルチキャスト方式では、以下の問題がある。

## 【 0 0 1 0 】

まず第1には、ネットワークの配信効率の低下を招くという問題が挙げられる。従来のマルチキャスト方式では、ネットワーク全体に対して情報の受け手を特定することなく配信し、ネットワーク上のエージェント全員が受信することとなる。これは、本来当該情報を受信する必要のないエージェントに対しても情報が毎回送信されることとなり、ネットワーク上に流されるデータ量が大きく、かつ、エージェント側の受信処理量も増大する。

## 【 0 0 1 1 】

第2には、セキュリティの低下を招くという問題が挙げられる。従来のマルチキャスト方式では、上述したようにネットワーク全体に対して情報の受け手を特定することなく配信し、ネットワーク上のエージェント全員が受信することとなる。そのため本来当該情報を配信すべきでない相手に対しても配信されることとなり、情報の漏洩を防止できない。このように配信経路を制御できないということとは即ち情報の到達性の保証に欠けるということでもある。

## 【 0 0 1 2 】

第3には、システム構成が固定的であり、動的な変更が困難であるという問題がある。従来のマルチキャスト方式では、エージェント連携をサーバが主体となっていくため、仲介する情報の内容や仲介処理内容に応じてサーバが異なるため、構築したシステムの変更が容易ではない。また、複数のサーバおよびエージェント間で情報のやり取りを行い、特定のサービスあるいは問題の解決を行うことを想定したとき、サーバあるいはエージェント間で情報を共有する必要がある。サーバあるいはエージェント間で情報を共有するためには、互いに情報をやり取

りするための通信路が必要であり、複数のサーバやエージェント間で情報交換するためのプログラムを個々のサーバやエージェント側で実装しておく必要が生じる。

#### 【 0 0 1 3 】

上記問題点に鑑み、本発明のエージェント連携システムは、要求やサービス内容に応じて情報を送受信する仮想通信路を柔軟かつ動的に定義付け、制御し、この仮想通信路を用いてエージェント間の連携を実現することを目的とする。この仮想通信路は、エージェント連携サービス開始にあたって動的に定義付け、提供され、エージェント連携サービス内容の変更に伴って動的に更新され、エージェント連携サービスの終了に伴って動的に解消・消滅するものとする。

#### 【 0 0 1 4 】

##### 【課題を解決するための手段】

上記目的を達成するために、本発明のエージェント連携システムは、エージェント間を仮想通信路により結んだエージェント連携システムであって、前記仮想通信路上の各エージェントが、エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーを記憶するポリシー記憶部を備え、前記ポリシーに従って各エージェントの属性に応じた権限を付与する権限付与部と、前記権限付与部により付与された権限および該権限内容が実行される条件を保持・記憶する権限・実行条件保持部と、前記権限内容の実行条件が成立した場合に該当する権限内容を実行する処理実行部を備え、前記ポリシーに従って前記仮想通信路を介して各エージェントが連携することを特徴とする。

#### 【 0 0 1 5 】

上記構成により、仮想通信路および仮想通信路上のエージェントが、ポリシーに規定されるエージェントの属性と権限との関係づけに従って動作し、エージェント間の動的な連携を実現することができる。

#### 【 0 0 1 6 】

なお、前記ポリシーは、エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールに加え、データオブジェクトが持つ属性とエージェ

ントから該データオブジェクトに対する操作に関する反応との関係を表わすルールと、前記権限の集合と前記反応の集合同士の関係を表わすルールと、前記権限の集合間の関係を表わすルールのいずれかまたはすべてを含むこととすれば、仮想通信路上のリソース、データの振る舞いをより柔軟に制御することができる。

## 【 0 0 1 7 】

なお、ポリシーの配布に関しては、エージェント自らが生成したポリシーを他のエージェントに配布し、前記配布されたポリシーを受け取った他のエージェントが、該ポリシーに従って前記権限付与部を用いてエージェントの属性に応じた権限を得て前記アクション実行部を構成し、前記配布されたポリシーを共通に持つエージェント間で仮想通信路を形成する仕組みとしても良く、また、前記仮想通信路上に前記ポリシーを記憶したポリシーリポジトリを備え、各エージェントが、前記ポリシーリポジトリから必要なポリシーを取り寄せ、前記ポリシー記憶部に記憶する仕組みとしても良い。

## 【 0 0 1 8 】

また、前記仮想通信路上に認証機構を備え、前記認証機構が、各エージェントの前記仮想通信路へのアクセス権の認証、各エージェントの権限保持部が保持する権限内容の認証を行うこととすれば、仮想通信路のセキュリティが向上する。例えば、前記認証機構が、ポリシー管理機関と、属性管理機関と、個体認証管理機関の3つの機関に分かれ、前記ポリシー管理機関が、ポリシーを記述したデータに対して電子署名を付し、真正のポリシーであることが認証されたポリシー証明書を発行し、前記属性管理機関が、各エージェントが持っている属性を証明した属性証明書を発行し、前記公開鍵管理機関が、ネットワーク上におけるエージェントの個体認証を行った証明である公開鍵証明書を発行し、各エージェントが、前記ポリシー証明書と属性証明書を解釈するトラストエンジンを備え、ネットワーク上で配布されたポリシー証明書と属性証明書に基づいて前記権限付与部に対して割り当てるべき適切な権限内容を指定する仕組みとしても良い。

## 【 0 0 1 9 】

このような認証システムを用いることにより、各エージェントが仮想通信路にログインする際に、前記トラストエンジンを用いて当該仮想通信路に対応するポ

リシーの証明書と属性証明書を入力としてポリシーの証明を得つつログインし、各エージェントのログインの連鎖により仮想通信路に参加するエージェント間にポリシーを安全に伝播させるということが可能となる。

#### 【 0 0 2 0 】

なお、前記ポリシー記憶部が前記相互独立に生成・管理している複数のポリシーのうち選択されたポリシーを統合し、統合後のポリシーに従って情報をやり取りするエージェント間の連携を前記仮想通信路に生成したり、前記ポリシーを複数相互独立に分割し、分割後のポリシーごとに、それぞれのポリシーに応じて情報をやり取りするエージェント間の連携を前記仮想通信路に相互独立に生成したりすることができる。

#### 【 0 0 2 1 】

次に、仮想通信路上のエージェント間連携の形態として、他のエージェントに対して要求を出すエージェントは、要求情報の送信にあたり、前記ポリシーに従って要求情報に前記ラベル情報を付して送信し、前記要求情報を受信し、前記要求に対する応答を実行した他のエージェントは、応答情報の送信にあたり、前記ポリシーに従って前記応答情報にラベル情報を付して送信し、前記要求を出したエージェントは、前記ポリシーに従って前記ラベル情報を持つ応答情報を受信するものとすることができ、ラベル情報を用いてエージェント間で要求・応答の連携を行うことができる。

#### 【 0 0 2 2 】

次に、本発明にかかる仮想通信路は、ネットワーク上に存在するエージェント間の情報通信を仲介する通信路であって、エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーに従って制御され、前記ポリシーに従って各エージェントに対してその属性に応じた権限を持たせ、前記ポリシーに従って動作するエージェント同士を仮想的に結び、前記権限内容の実行を通して各エージェントの連携処理を仲介することを特徴とする。

#### 【 0 0 2 3 】

上記の仮想通信路を構築することにより、仮想通信路上のエージェントが、ポ

リシーに規定されるエージェントの属性と権限との関係づけに従って動作するようにエージェント間の動的な連携を与えることができる。

【 0 0 2 4 】

本発明のエージェント連携システムを実現する処理プログラムを記録したコンピュータ読み取り可能な記録媒体を提供すれば、当該記録媒体をコンピュータに読み取ることにより、コンピュータ装置を利用して本発明のエージェント連携システムを構築することができ、エージェント間に仮想通信路を柔軟かつ容易に構築、更新することができるエージェント連携システムを構築できる。

【 0 0 2 5 】

#### 【発明の実施の形態】

以下、本発明のエージェント連携システムの実施形態について、図面を参照しながら説明する。

【 0 0 2 6 】

#### （実施形態 1）

実施形態 1 のエージェント連携システムは、ネットワーク上のエージェント間の仮想通信路を制御するシステムであって、仮想通信路上の各エージェントが、エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーに従って各エージェントの属性に応じた権限を持ち、メッセージ受信など権限内容の実行条件が成立した場合に、該当する権限内容を実行することにより、各エージェントを連携させる。本発明の仮想通信路は、上記ポリシーに従って制御され、ポリシーに従ってエージェント同士を仮想的に結び、連携を仲介する。

【 0 0 2 7 】

以下、本発明のエージェント連携システムの実施形態として、最初に本発明におけるポリシー、エージェントの持つ属性に応じて割り当てられる権限（ロール）、データオブジェクトのラベル情報について述べ、エージェント連携システムの装置構成例とその動作例、仮想通信路の動的な生成、変更、消滅の様子を説明する。

【 0 0 2 8 】

まず、本発明におけるポリシー、エージェントの権限（ロール）、データオブジェクトのラベル情報の定義およびそれらの関係について述べる。

#### 【 0 0 2 9 】

ポリシーとは、仮想通信路上におけるエージェントやデータオブジェクトなどのリソースの動作・性質・関係を記述したルールの集合であり、エージェント達の連携により構築される仮想通信路の動作・性質・関係を記述したルールと言える。このようにポリシーとして記述されるルールは多様なものがある。例えば、エージェントが持つ属性と、それら属性に対応して割り当てられる仮想通信路上での操作や動作などに関する権限の集合（ロール）の関係を記述したルールがある。また、データオブジェクトが持つ属性と、それら属性に対応して割り当てられる仮想通信路上でのエージェントからの操作等に対応する反応の集合（ラベル）との関係を記述したルールがある。また、上記したエージェントの持つ権限の集合（ロール）とデータオブジェクトの反応の集合（ラベル）の間の関係を記述したルールがある。また、上記したエージェントの持つ権限の集合（ロール）と権限の集合（ロール）同士の関係を記述したルールもある。さらに、本発明の仮想通信路自体、参加するエージェント達自身のネットワークで構成されているので、仮想通信路の生成・変更・消滅に関してもエージェントの動作の一環として記述することができる。このように、ポリシーには仮想通信路の生成・変更・消滅を含む仮想通信路そのものの動作に関するルールも含まれる。

#### 【 0 0 3 0 】

なお、このポリシーは、後述する他の実施形態 4 に示すようにポリシーリポジトリサーバというポリシーを集中的に管理するサーバをネットワーク上に用意して管理し、各エージェントが取り寄せる仕組みでも良く、また、各エージェント自らが生成・証明したポリシーをネットワーク上に配布し、当該ポリシーを受け取り（契約し）、当該ポリシーに従ってロールを得たエージェント間で仮想通信路を形成する仕組みとしても良い。後者は仮想通信路を用いた完全自立分散型のエージェント連携と言える。例えば、エージェント自らが管理する画像データベースのコンテンツ配布をサービスしたいエージェントが、一定の料金を支払うという契約を結んだエージェントであるという属性と、該画像データベースコンテ

ンツをダウンロードするという権限との関係を記述したルールをポリシーとし、該ポリシーをネットワーク上に配布するなどという利用が想定できる。

#### 【 0 0 3 1 】

ポリシーの実例を図 1 に示す。図 1 は、ポリシー記述の一例を示す図である。簡単な画像イメージ配送サービスに関するポリシー例を示した。1 は、ポリシーとして配布されるべきファイルなどを記述している。ここで、“image.jar” はロール（権限内容）を実行するプログラムモジュールであるロールプログラムファイル、“image.xml” は本ポリシー記述ファイルを指している。2 は、ロール割り当てのためのルール群である。まず最初にロール割り当てのための条件、即ち、属性とその値の指定（図中 3）を記述し、続いてそれが満たされた場合に割り当てられるロールが記述される（図中 4）。図 1 のポリシーの例では、まず登録料の支払いについて属性に注目し、登録料を支払っていれば登録ユーザのロール（権限内容）が与えられる。逆に支払っていない場合はルールの第 3 項目に定義されているように未登録ユーザ用のロール（権限内容）が与えられる。また、画像イメージコンテンツの提供者になるかどうかの契約に着目すると、契約を行った場合には画像イメージコンテンツの提供者としてのロール（権限内容）が与えられる。このようなポリシー記述を持つポリシーを用意し、各エージェントが装備することにより、ポリシー記述に従って制御される仮想通信路を生成することができる。

#### 【 0 0 3 2 】

なお、エージェントのロールとは、上記にも述べたように、エージェントの属性に応じて割り当てられた権限の集合である。エージェントは付与された権限に応じて動作し、動作の一環として他のエージェントとの連携処理を実行する。ロールには実行できる権限内容が決められており、また、当該権限内容を実行するための実行条件が決められている。ここで実行条件とは、例えば、仮想通信路から特定のメッセージを受信することや、エージェントのステータスが特定の状態になったことや、あるイベントが起こった場合、あるイベントから一定時間が経過した場合など多様な条件がある。

#### 【 0 0 3 3 】



データオブジェクトのラベル情報とは、上記にも述べたように、データオブジェクトの属性に対応して割り当てられるエージェントからの操作等に対応する反応の集合である。例えば、一定権限を持つエージェントからのデータ内容の読み出し操作、書き込み操作、削除操作を認めることや、一定権限を持つエージェントによる演算操作、検索操作、転送操作を認めることなどがある。

#### 【 0 0 3 4 】

次に、エージェント連携システムの装置構成例について説明する。

#### 【 0 0 3 5 】

図2は、エージェント連携システムの装置構成例を模式的に示す図であり、一つのエージェントの内部構成例を示した。本発明のエージェント連携システムは、図2に示した構成を持つ複数のエージェントがネットワークを介して連携し合うシステムであり、本発明の仮想通信路は、これらエージェント間を結ぶネットワーク上に仮想的に形成される連携の場、コミュニケーションの場と言える。

#### 【 0 0 3 6 】

図2において、100はエージェントであり、200は外部ネットワーク、210は内部フィールドである。10はエージェントネットワークコネクタ、20はセキュリティマネージャ、30はロールマネージャ、40は属性マネージャ、50はロールプログラムデータベース、60はフィールドコネクタ、70はロールメソッドテーブル、80はロール実行部である。

#### 【 0 0 3 7 】

上記のエージェント100の構成において、セキュリティマネージャ20、ロールマネージャ30、属性マネージャ40、ロールプログラムデータベース50は、ポリシーに従って内部フィールド210の生成、変更、消滅を実行するためのモジュールである。また、上記エージェント100は、フィールドコネクタ60を持っている。セキュリティマネージャ20はフィールドコネクタ60上に内部フィールド210を構築する。さらに、ロールマネージャ30、属性マネージャ40が内部フィールド210につながるロールメソッドテーブル70、ロール実行部80をそれぞれ構成する。図2の例では3つの内部フィールド210a～c、ロールメソッドテーブル70a～c、ロール実行部80a～cが構築されている。

## 【 0 0 3 8 】

なお、内部フィールド 2 1 0、ロールメソッドテーブル 7 0、ロール実行部 8 0 は、権限実行条件が成立した場合に権限内容（アクション）の実行を行うためのモジュールである。例えば外部ネットワーク 2 0 0 から特定のメッセージを受信したことを条件として対応するロールを反応させ、実行する。

## 【 0 0 3 9 】

各モジュールを説明する。

## 【 0 0 4 0 】

ネットワークエージェントコネクタ 1 0 は、エージェント 1 0 0 と外部ネットワーク 2 1 0 とを接続する通信インタフェースを提供する部分である。メッセージを外部ネットワーク 2 0 0 から受け取り、メッセージの種類に応じて該メッセージをセキュリティマネージャ 2 0 に渡すかフィールドコネクタ 6 0 に渡すかを振り分ける。受け取ったメッセージが、フィールド生成メッセージやフィールド検索メッセージやフィールド削除メッセージなどフィールドの生成、変更、消滅に関わるメッセージであればセキュリティマネージャ 2 0 に振り分け、メッセージがエージェント連携に関するフィールドメッセージであればフィールドコネクタ 6 0 に振り分ける。

## 【 0 0 4 1 】

セキュリティマネージャ 2 0 は、フィールドの生成、変更、消滅に関わるメッセージを受け取ると該メッセージの正当性を確認する機能と、該メッセージ内容を解釈し、フィールドの生成、変更、消滅の指示に応じて内部フィールド 2 1 0 の生成、変更、消滅を実行する機能と、該メッセージからポリシーを抽出する機能を有する。メッセージの正当性を確認する機能は本発明のエージェント連携システムのセキュリティ向上のために必要な機能である。内部フィールド 2 1 0 の生成、変更、消滅を実行する機能に関しては、フィールドコネクタ 6 0 は生成された内部フィールド 2 1 0 と外部ネットワーク 2 0 0 を接続するポイントとなるものであり、その生成、変更、消滅は、セキュリティマネージャ 2 0 が実行することとしている。なお、メッセージからポリシーを抽出する機能により図 1 に示されたようなポリシーが抽出され、ロールマネージャ 3 0 に渡される。

## 【0042】

ロールマネジャ30は、セキュリティマネジャ30から受け取ったポリシーを解釈し、エージェントが持つ属性と照合を行い、ロール生成、消滅を制御する。ポリシーの中の各ルールの特徴部に指定された属性とその値と、エージェントが持つ属性とその値を参照するため、属性マネジャ40に対して属性とその値を問い合わせを行う。属性マネジャ40からの回答を得て、ルールの条件を満足する場合にはロールメソッドテーブル70に対してロール名を通知し、ロールメソッドテーブル70の構築、内容の変更を指示する。なお、ロールマネジャ30はポリシーを記憶しておくポリシー記憶部31を備え、ポリシーを格納しておく。

## 【0043】

属性マネジャ40は、属性データベース41を備えている。属性マネジャ40は、ロールマネジャ30からのエージェントが持つ属性とその値の問い合わせに対して、属性データベース41を参照して該問い合わせに対して回答する。

## 【0044】

ロールプログラムデータベース50は、ロール実行部80を構築するためのプログラムを格納したデータベースであり、ロール実行部80の構築時にロールマネジャ30の制御により必要なプログラムが取り出され、ロール実行部80の構築に供される。なお、このロールプログラムは、ネットワークを介した外部に存在するものであっても良く、必要に応じてアクセスし、ロールプログラムをダウンロードできる仕組みであれば良い。

## 【0045】

内部フィールド210は、その生成、変更、消滅に関しては、セキュリティマネジャ20からの指示により生成、変更、消滅される。内部フィールド210の生成指示があれば、フィールドコネクタ60上に新しい内部フィールドが生成される。同様に存在している内部フィールド210の消滅指示があれば、フィールドコネクタ60が内部フィールド210を消滅させる。次に、メッセージ受信など権限実行条件の成立による権限内容の実行処理に関しては、まず、フィールドコネクタ60は、エージェントネットワークコネクタ10からフィールドメッセージを受け、フィールドメッセージの内容や属性を調べ、適切なフィールドコネ

クタ 6 0 のみが内部フィールド 2 1 0 に対して当該メッセージを流す。また、ロール実行部 8 0 の実行処理の一環として返される応答メッセージなどを受け、該応答メッセージをエージェントネットワークコネクタ 1 0 を介して外部ネットワーク 2 0 0 に対して発信する。

#### 【 0 0 4 6 】

ロールメソッドテーブル 7 0 は、ロールマネージャ 3 0 からの指示を受け、テーブルの構築、その内容の変更を行う。内部フィールドの生成に際しては、ロールマネージャ 3 0 からロール名の通知を受けて、ロールプログラム集より適切なロールを呼び出し、指定されたロールに応じたメソッドを関係づけて格納する。また、当該ロールが起動されるための実行条件を関係づけてテーブルに格納しておく。次に、メッセージ受信など権限実行条件の成立による権限内容の実行処理に関しては、フィールドメッセージの受信や、各種イベントの発生、エージェントステータスの変更などの条件を検知したフィールドコネクタ 6 0 から、該条件を実行条件に持っているロールがあるか否かの問い合わせを受け、該当するロールがある場合にはそのロールを制御するメソッドを指定し、フィールドコネクタ 6 0 に通知する。

#### 【 0 0 4 7 】

次に、ロール実行部 8 0 は、ロールマネージャ 3 0 からの指示を受け、ロールプログラムデータベース 5 0 から適切なロールを呼び出して、格納しておく。次に、メッセージ受信など権限実行条件の成立による権限内容の実行処理に関しては、フィールドメッセージに従い、フィールドコネクタ 6 0 により特定のメソッドが起動されると該メソッドに対応するロール内容を実行する。逆に、実行条件が成り立たなくなれば、該メソッド制御のもと対応するロール実行が停止される。

#### 【 0 0 4 8 】

以上に示した構成例のエージェント連携システムの動作を図 3 のフローチャートを参照しつつ説明する。以下の例では、ロール実行条件として特定のフィールドメッセージを受信することをロールの実行条件とした例を説明する。なお、図 3 のフローチャートにおいて説明の便宜上、エージェントネットワークコネクタを ANC、フィールドコネクタを FC、セキュリティマネージャを SM、ロールマ

ネ ज्याを RM、属性マネ ज्याを AM と記号で略記した。

【 0 0 4 9 】

まず、エージェントネットワークコネクタ 1 0 が外部ネットワーク 2 0 0 をモニタし、データ受信を待っている（ステップ S 3 0 1）。

【 0 0 5 0 】

外部ネットワーク 2 0 0 からデータを受信すると（ステップ S 3 0 1 : Y）、エージェントネットワークコネクタ 1 0 は、該データがフィールドメッセージか否かをチェックする（ステップ S 3 0 2）。

【 0 0 5 1 】

該データがフィールドメッセージである場合（ステップ S 3 0 2 : Y）、エージェントネットワークコネクタ 1 0 は、フィールドメッセージからフィールド名を取り出し、該当するフィールドコネクタ 6 0 へ転送する（ステップ S 3 0 3）。

【 0 0 5 2 】

フィールドコネクタ 6 0 は、ロールメソッドテーブル 7 0 を参照し、該メッセージ受信を実行条件としているロールを検索する（ステップ S 3 0 4）。対応するロールが存在する場合（ステップ S 3 0 4 : Y）は、該ロールの実行を制御するメソッドが起動され、ロールが実行され（ステップ S 3 0 5）、ステップ S 3 0 1 に戻る。対応するロールが存在しない場合（ステップ S 3 0 4 : N）、ロールは何も反応せず実行されずステップ S 3 0 1 に戻る。

【 0 0 5 3 】

次に、ステップ S 3 0 2 において、受信データがフィールドメッセージでない場合（ステップ S 3 0 2 : N）、エージェントネットワークコネクタ 1 0 は、データをセキュリティマネ ज्या 2 0 に転送し、セキュリティマネ ज्या 2 0 は受信データが新しいフィールド生成メッセージであるか否かをチェックする（ステップ S 3 0 6）。

【 0 0 5 4 】

受信データが新しいフィールド生成メッセージである場合（ステップ S 3 0 6 : Y）、セキュリティマネ ज्या 2 0 は、受信メッセージからポリシーを取り出し

、ロールマネジャ 3 0 へ転送する（ステップ S 3 0 7）。ロールマネジャ 3 0 はポリシーに記述されている属性およびその値に関し、属性マネジャ 4 0 に問い合わせ、属性マネジャ 4 0 からの応答結果からエージェントに与えられるロールを決定する（ステップ S 3 0 8）

ロールマネジャ 3 0 は、フィールド生成メッセージに対応して、フィールドコネクタ 6 0 を生成し、該フィールドコネクタに構築すべきロール名とその内容を通知する（ステップ S 3 0 9）。ロールマネジャ 3 0 は、通知されたロール内容を構築するため、ロールプログラム集から該当するロールをロール実行部 8 0 にロードし、必要なロール実行モジュールを構築し、内部フィールド 2 1 0 を生成する（ステップ S 3 1 0）。このように内部フィールド 2 1 0 が生成されれば、適切にステップ S 3 0 1 に戻る。

#### 【 0 0 5 5 】

次に、ステップ S 3 0 6 において、受信データが新しいフィールド生成メッセージでない場合（ステップ S 3 0 6 : N）、受信データがフィールド検索メッセージであるか否かをチェックする（ステップ S 3 1 1）。受信データがフィールド検索メッセージである場合（ステップ S 3 1 1 : Y）、セキュリティマネジャ 2 0 はメッセージ内容からフィールド検索条件を抽出し、検索条件に該当するフィールド名をエージェントネットワークコネクタ 1 0 を介して検索元に対して返信する（ステップ S 3 1 2）。返信後、適切にステップ S 3 0 1 に戻る。

#### 【 0 0 5 6 】

受信データがフィールド検索メッセージでない場合（ステップ S 3 1 1 : N）、セキュリティマネジャ 2 0 は、受信メッセージがフィールド削除メッセージであるか否かをチェックする（ステップ S 3 1 3）。受信メッセージがフィールド削除メッセージである場合（ステップ S 3 1 3 : Y）、セキュリティマネジャ 2 0 は、フィールド削除メッセージから削除すべきフィールド名を抽出し、該当するフィールドのフィールドコネクタ 6 0 に対してフィールドの削除を通知する（ステップ S 3 1 4）。フィールドの削除を通知されたフィールドコネクタ 6 0 は、管理する内部フィールド 2 1 0 を削除する（ステップ S 3 1 5）。なお、内部フィールド 2 1 0 の消滅に伴って対応するロールメソッドテーブル 7 0、ロール

実行部 8 0 が消滅する。フィールド削除後、適切にステップ S 3 0 1 に戻る。

【 0 0 5 7 】

受信メッセージがフィールド削除メッセージでない場合（ステップ S 3 1 3 : N）、この例では、受信データに対する有効な応答が行われず、ステップ S 3 0 1 に戻って、次のデータ受信を待つ。

【 0 0 5 8 】

以上が、本実施形態 1 のエージェント連携システムによる仮想通信路の生成、変更、消滅、生成された仮想通信路を用いたエージェント連携動作の流れの一例である。

【 0 0 5 9 】

本実施形態 1 のエージェント連携システムは、以上に見たように、本発明のエージェント連携システムおよびエージェント間を結ぶ仮想通信路は、エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーに従って制御され、ポリシーに従ってポリシーに従ってエージェント同士を仮想的に結び、エージェント間の連携を仲介できる。

【 0 0 6 0 】

（実施形態 2）

実施形態 2 では、本発明のエージェント連携システムにおいて、エージェント間の連携の形態ついてバリエーションを持たせるように仮想通信路を定義付け、制御することができることを説明する。

【 0 0 6 1 】

なお、エージェント連携システムの装置構成例は図 2 で示したものと同様であるのでここでの説明は省略する。

【 0 0 6 2 】

第 1 に、本発明のエージェント連携システムにおいて、エージェント間の連携を複数相互独立な形態で構築することが可能である。この場合、セキュリティマネージャ 2 0、ロールマネージャ 3 0 が、ポリシーに従い、複数相互独立の内部フィールド 2 1 0 を生成・管理し、ロール実行により各エージェントが連携することにより、複数相互独立のエージェント連携関係が仮想通信路上に構築される。こ

の複数相互のエージェント間連携の構築の様子を概念的に示したものが図 4 (a) である。

【 0 0 6 3 】

第 2 に、本発明のエージェント連携システムにおいて、複数相互独立な形態で構築されているエージェント間の連携を統合することが可能である。この場合、セキュリティマネジャ 2 0、ロールマネジャ 3 0 が相互独立に生成・管理している複数の内部フィールド 2 1 0 のうち選択したものを統合する指示を出すことにより、対応するフィールドコネクタが 1 つのフィールドコネクタとして再生成され、内部フィールドも 1 つのものが再生成され、既存の 2 つの相互独立のエージェント間連携を統合した形のエージェント間の連携が生成される。この複数相互のエージェント間連携を統合する様子概念的に示したものが図 4 (b) である。

【 0 0 6 4 】

第 3 に、本発明のエージェント連携システムにおいて、既存のエージェント間の連携を分割することが可能である。この場合、セキュリティマネジャ 2 0、ロールマネジャ 3 0 が、分割後の一方のフィールドと他方のフィールドのそれぞれの生成指示を出すことにより、対応するそれぞれのフィールドコネクタが生成され、それぞれの内部フィールドも生成される。このエージェント間連携を分割する様子概念的に示したものが図 4 (c) である。

【 0 0 6 5 】

第 4 に、本発明のエージェント連携システムにおいて、エージェント間連携を親として、いわゆる入れ子状態で、子に相当するエージェント連携を構築することも可能である。この場合、セキュリティマネジャ 2 0、ロールマネジャ 3 0 が、親のフィールド生成指示と子のフィールド生成指示を出し、親フィールドと子フィールドが生成される。このエージェント間連携の入れ子状態の様子概念的に示したものが図 4 (d) である。

【 0 0 6 6 】

以上に示すように、本発明のエージェント連携システムは、ポリシーに従って構築するエージェント間の連携の形態についてバリエーションを持たせることがで



きる。

【0067】

(実施形態3)

実施形態3のエージェント連携システムとして、ポリシーの真正性確保のためのポリシー証明、ロールの真正性確保のためのロール保証、完全自立分散構成の場合におけるログインの連鎖による安全なポリシー配布、不正アクセスに対する処理、エージェント連携の確認などに関し、セキュリティ向上を図った構成例を示す。

【0068】

まず、ポリシーの真正性確保のためのポリシー証明、ロールの真正性確保のためのロール保証を説明し、各エージェントにおいて、証明された真正なポリシーを受け、正しく保証されたロールが割り当てられ、仮想通信路に参加する仕組みを説明する。

【0069】

図5は、ポリシーの真正性確保のためのポリシー証明、ロールの真正性確保のためのロール保証を行う概念を模式的に示した図である。図5において、5は、ポリシー証明書の発行主体となる権威機関であるポリシー管理機関(policy approving authority: PAA)、6は、属性証明書の発行主体となる権威機関である属性管理機関(attribute authority: AA)、7は、個体認証を行い、公開鍵証明書の発行主体となる権威機関である個体認証機関(certification authority: CA)である。このように3つの権威機関を設けることにより、ポリシー認証、属性認証、個体認証という3つの側面についてそれぞれ異なる権威機能を分散して設け、広域分散環境などにおける仮想通信路の構築、仮想通信路を用いた情報のやり取りについて高いセキュリティを持たせることを狙っている。

【0070】

ここで、ポリシー証明書とは、ポリシーを記述したデータに対して電子署名を付したものである。つまりネットワークに正当に配布された真正のポリシーであることが認証されているものである。このポリシー証明書は、ネットワークを介してエージェントなどに配布される。あるポリシー証明書によって同一のポリシ

ーが伝播している仮想的なネットワーク領域が信用ドメインとなり、仮想通信路によって形成されるコミュニケーション空間とも言える。新しいエージェントがある信用ドメインに加わり仮想通信路に参加しようとする場合にはまず、対応するポリシー証明書を受け取り、その内容に合意してポリシー証明書に基づいた権限割り当てを受ける必要がある。

#### 【0071】

属性証明書とは、個人の属性を認証する属性管理機関6が、各エージェントが持っている属性を証明したものを言う。例えば、ITU-TX. 509属性証明書に準じた形で記述される。なお、属性管理機関6による属性証明書の発行にあたっては、図2に示した各エージェントが持つ属性管理データベース50に対してアクセスし、各エージェントが持っている属性を参照することができる。

#### 【0072】

公開鍵証明書とは、ネットワーク上における本人認証を行うものであって、個体認証を行う権威機関である個体認証機関7により、例えば、ITU-TX. 509公開鍵証明書などの公開鍵認証基盤に基づいて発行される。

#### 【0073】

次に、各エージェントにおいて、証明された真正なポリシーを受け、正しく保証されたロールが割り当てられる仕組みを説明する。

#### 【0074】

図5において、8は、各エージェントが実装するトラストエンジンであって、ネットワーク上で伝播されているポリシー証明書や属性証明書を入力として解釈し、それらポリシー証明書や属性証明書に対応した適切なロールを特定して割り当てるものである。なお、この各エージェントが実装するトラストエンジンは、実施形態1で図2を用いて説明した各エージェント構成において、ロールマネージャ30および属性マネージャ40による複合機能として構成される。

#### 【0075】

本実施形態3の認証システムでは、各エージェントがこのトラストエンジン8を実装し、ポリシー管理機関5、属性管理機関6、個体認証機関7を信頼し、発行されているポリシー証明書や属性証明書をトラストエンジン8により安全に解

釈し、ロールの割り当てを実行する。この割り当てられたロールにはロール保証書が付され、ロールの正当性が保証される。なお、トラストエンジン自体の正当性は、例えば、公開鍵認証基盤に基づく、SSLによる相互認証とオブジェクト署名の検証によって証明でき、従ってこのトラストエンジンにより生成されたロール保証書の正当性も保証される。

【0076】

このように生成されたロール保証書に基づいて、各エージェントにおいて、ロールマネージャの制御のもと、ロールが割り当てが実行される。

【0077】

以上の認証システムに基づいて、ポリシー証明、ロール保証が実行され、高いセキュリティのもと、仮想通信路が生成・制御され、各エージェントが該仮想通信路に安全に出入りできる。

【0078】

次に、完全自立分散構成の場合におけるログインの連鎖による安全なポリシー配布について説明する。同一のポリシーが伝播している仮想通信路上の参加エージェントは任意に出入りが可能でありその参加者は動的に変化する。本発明の仮想通信路を制御するエージェント連携システムを分散型システムとして構築した場合には、真正が保証された集中管理用の特定のエージェントが存在しないので、新しく仮想通信路に参加しようとするエージェントは、既に参加済みの任意のエージェントに対してログインの要求を行うこととなる。各エージェントによる仮想通信路へのログインは、上記図5に見たように、各エージェントが持つ属性情報とポリシーに基づいて行われ、ログインの結果としてエージェントにはロールが割り当てられる。ここで、ログイン時にロール割り当て処理を行うトラストエンジン8は、既に信用ドメインに参加しているエージェントに稼動しているものではなく、新規に参加しようとしているエージェント側で稼動しているものを使用することがポイントとなる。これにより、一種のプライバシー情報と言える属性情報を他に通知することなく、かつ、仮想通信路全体のセキュリティを低下させることなく安全にログイン処理を行うことができる。このような個々のエージェントのログインの連鎖によって、集中管理システムなしにログインを介し

てポリシーを安全に伝播させることができ、各エージェントは仮想通信路に対して任意にログイン、ログアウトすることができる。

#### 【 0 0 7 9 】

次に、不正アクセスや、参加者からの要望に応じて仮想通信路を消滅させる処理について説明する。これは、エージェント間でメッセージが所定通りにやり取りされ、連携が正常に実行されているか、さらに、不正なアクセスがないかについてチェックし、不正なアクセスがあった場合に動的に仮想通信路を無効化するものである。図6は、エージェント間でのメッセージのやり取りの確認、不正アクセス検知を実行するエージェント連携システムの構成例を示す図である。実施形態1で説明した図2の構成と同様の部分についてはここでは説明を省略する。

#### 【 0 0 8 0 】

図6に示すように、エージェント100aは、エージェント連携確認部90を備えている。また、各エージェントは処理機能の一つとしてメッセージを受信した場合に受領通知を仮想通信路上に返す仕組みとする。エージェント連携確認部90は、エージェントネットワークコネクタ10を介して仮想通信路上に送信されているメッセージをモニタし、あるエージェントから流された依頼メッセージを確認する。その後、モニタを続け、当該依頼メッセージを受領した他のエージェントから当該依頼メッセージを受信した旨の受領通知メッセージをモニタして依頼メッセージの受信を確認する。このように、エージェント連携確認部90を用いて仮想通信路上で送信されたメッセージとそのメッセージに対する受領通知をモニタすることにより、エージェント間の情報の仲介が正常に実行され、エージェントの連携が正常に実行されていることを確認する。

#### 【 0 0 8 1 】

エージェントネットワークコネクタ10は、アクセス権管理部11と不正アクセス検知部12を備えている。

#### 【 0 0 8 2 】

不正アクセス検知部12は、仮想通信路に対する不正アクセスを検知する部分である。不正を検知する方法は種々あるが、例えば、アクセス権管理部11が管理しているアクセス権の内容に違反してエージェントがアクセスし、メッセージ

を送受信していれば、不正アクセス検知部 1 2 は、不正アクセスがあったことを検知する。また、例えば、不正アクセス検知部 1 2 は、メッセージの改ざんを検知する機能を有している。電子署名がメッセージに埋め込まれている場合に電子署名が壊れていないかチェックしたり、電子透かしが埋め込まれている場合に電子透かしに異常が見られないかチェックしたり、ロールに相応しくないメッセージを受信したことをチェックしたり、データオブジェクトがアクセスしてきたエージェントの資格に合わないメソッドでアクセスされていないかチェックしたりすることにより不正アクセスを検知する。

## 【 0 0 8 3 】

不正アクセス検知部 1 2 は不正アクセスを検知すれば、セキュリティマネージャ 2 0 にフィールドの消滅指示を通知し、セキュリティマネージャ 2 0 が不正アクセスが試みられた内部フィールドを消滅させ、外部ネットワーク 2 0 0 との接続を遮断する。

## 【 0 0 8 4 】

なお、上記の仮想通信路の消滅は、自発的にエージェント側からも請求しうる構成とすることができる。例えば、ロール実行部 8 0 のロールなどが仮想通信路を消滅させたい旨の要求を出した場合、フィールドコネクタ 6 0 を介してエージェントネットワークコネクタ 1 0 に通知され、エージェントネットワークコネクタ 1 0 がセキュリティマネージャ 2 0 に対して該当する仮想通信路の消滅指示を出す。セキュリティマネージャ 2 0 は対応する内部フィールドを消滅させる。

## 【 0 0 8 5 】

また、仮想通信路に対して有効期限を設けておき、仮想通信路を消滅させることもできる。例えば、セキュリティマネージャ 2 0 またはフィールドコネクタ 6 0 がタイマを備え、タイマにより有効期限に到達したか否かを検知し、有効期限の経過が検知されればセキュリティマネージャ 2 0 の消滅指示を受けて対応する内部フィールド 2 1 0 が消滅され、または、有効期限に到達したことを検知したフィールドコネクタ 6 0 が自動的に該当する内部フィールド 2 1 0 を消滅させる。

## 【 0 0 8 6 】

また、本発明のエージェント連携システムはエージェント間でやりとりするメ

ッセージを暗号化することによりセキュリティを向上することも可能である。相互に送信メッセージの暗号化処理機能と、受信メッセージの復号化処理機能を有し、メッセージの送受信にあたりメッセージの暗号化復号化処理を実行する。どの暗号鍵、復号鍵を用いるかについては、例えば、用いられるルールに基づいて決定することができる。

## 【 0 0 8 7 】

以上、実施形態 3 のエージェント連携システムは、ポリシーの真正性確保のためのポリシー証明、ロールの真正性確保のためのロール保証、エージェント間連携でのメッセージのやり取りの暗号復号化、各エージェントによる仮想通信路へのアクセス権の管理、不正アクセスに対する処理、エージェント連携の確認などに関し、セキュリティ向上を図ることができる。

## 【 0 0 8 8 】

## (実施形態 4)

実施形態 4 のエージェント連携システムは、ポリシーの頒布に関し、ポリシーリポジトリサーバを備えたものである。

## 【 0 0 8 9 】

図 7 は、本実施形態 4 にかかるポリシーリポジトリサーバを備えたエージェント連携システムの構成例である。3 0 0 は、ポリシーリポジトリサーバであり、複数のポリシーが格納されている。

## 【 0 0 9 0 】

エージェント 1 0 0 が仮想通信路を構築または既存の仮想通信路に参加する場合、エージェントは対象となる仮想通信路を記述したポリシーを得て、当該ポリシーに従ってロールを構築しなければならない。エージェント 1 0 0 はポリシーリポジトリサーバ 3 0 0 にアクセスし、対象となるポリシーの送信を依頼する。ポリシーリポジトリサーバ 3 0 0 は、格納しているポリシーから該当するポリシーを依頼元のエージェント 1 0 0 に送信する。ポリシーの頒布を受けたエージェント 1 0 0 は、エージェントネットワーク 1 0 を介してセキュリティマネジャ 2 0 に渡され、セキュリティマネジャ 2 0 がポリシーを抽出し、ロールマネジャ 3 0 にポリシーを渡し、ロールマネジャ 3 0 はポリシーをポリシー記憶部 3 1 に格

納する。セキュリティマネージャ 2 0 およびロールマネージャ 3 0 が、受け取ったポリシーに従って該当する内部フィールドを構築する点については実施形態 1 と同様である。

#### 【 0 0 9 1 】

以上、本発明のエージェント連携システムは、ポリシーを一元的に管理し、頒布するポリシーリポジトリサーバを備え、未だポリシーを持っていないエージェントに対するポリシーの頒布を実行でき、また、ポリシーそのものの更新がある場合においてエージェントに対して更新後のポリシーを頒布することができる。

#### 【 0 0 9 2 】

##### (実施形態 5)

本発明のオブジェクトエージェント連携システムは、上記に説明した構成を実現する処理ステップを記述したプログラムをコンピュータ読み取り可能な記録媒体に記録して提供することにより、各種コンピュータを用いて構築することができる。本発明のオブジェクトエージェント連携システムを実現する処理ステップを備えたプログラムを記録した記録媒体は、図 8 に図示した記録媒体の例に示すように、CD-ROM 1 0 0 2 やフレキシブルディスク 1 0 0 3 等の可搬型記録媒体 1 0 0 1 だけでなく、ネットワーク上にある記録装置内の記録媒体 1 0 0 0 や、コンピュータのハードディスクや RAM 等の記録媒体 1 0 0 5 のいずれであっても良く、プログラム実行時には、プログラムはコンピュータ 1 0 0 4 上にローディングされ、主メモリ上で実行される。

#### 【 0 0 9 3 】

さらに、ソースプログラムをコンパイルしたもののみならず、いわゆるネットワークを介してクライアントコンピュータに中間言語形式のアプレットを送信し、クライアントコンピュータ上でインタプリタ実行して動作する構成であっても良い。

#### 【 0 0 9 4 】

本発明の仮想通信路および仮想通信路を制御するエージェント連携システムおよびエージェント連携方法において、さらに以下の項を開示する。

#### 【 0 0 9 5 】

（付記 1）エージェント間を仮想通信路により結んだエージェント連携システムであって、前記仮想通信路上の各エージェントが、

エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーを記憶するポリシー記憶部を備え、前記ポリシーに従って各エージェントの属性に応じた権限を付与する権限付与部と、

前記権限付与部により付与された権限および該権限内容が実行される条件を保持・記憶する権限・実行条件保持部と、

前記権限内容の実行条件が成立した場合に該当する権限内容を実行する処理実行部を備え、

前記ポリシーに従って前記仮想通信路を介して各エージェントが連携することを特徴とするエージェント連携システム（1）。

【 0 0 9 6 】

（付記 2）前記ポリシーが、エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールに加え、データオブジェクトが持つ属性とエージェントから該データオブジェクトに対する操作に関する反応との関係を表わすルールと、前記権限の集合と前記反応の集合同士の関係を表わすルールと、前記権限の集合間の関係を表わすルールのいずれかまたはすべてを含む付記 1 に記載のエージェント連携システム（2）。

【 0 0 9 7 】

（付記 3）各エージェントにおいて、前記ポリシー記憶部に記憶されているポリシーの内容を更新し、前記ルールの消去、変更、新たなルールの追加を行うことができる付記 1 に記載のエージェント連携システム。

【 0 0 9 8 】

（付記 4）前記処理実行部が予め処理機能モジュールを保持し、前記権限保持部が保持する権限内容に沿って、前記処理実行部に含まれる処理機能モジュールを選択的に有効化して処理機能を構築する付記 1 に記載のエージェント連携システム。

【 0 0 9 9 】

（付記 5）前記処理実行部における処理機能の構築において、前記権限内容の



実行に必要な処理機能モジュールが予め保持されていない場合、前記仮想通信路を介してネットワーク上のリソースから必要な処理機能モジュールを受信して利用する付記 4 に記載のエージェント連携システム。

【 0 1 0 0 】

（付記 6）エージェント自らが生成したポリシーを他のエージェントに配布し、

前記配布されたポリシーを受け取った他のエージェントが、該ポリシーに従って前記権限付与部を用いてエージェントの属性に応じた権限を得て前記アクション実行部を構成し、

前記配布されたポリシーを共通に持つエージェント間で仮想通信路を形成する付記 1 に記載のエージェント連携システム（3）。

【 0 1 0 1 】

（付記 7）前記仮想通信路上に前記ポリシーを記憶したポリシーリポジトリを備え、

各エージェントが、前記ポリシーリポジトリから必要なポリシーを取り寄せ、前記ポリシー記憶部に記憶する付記 1 に記載のエージェント連携システム。

【 0 1 0 2 】

（付記 8）前記仮想通信路上に認証機構を備え、

前記認証機構が、各エージェントの前記仮想通信路へのアクセス権の認証、各エージェントの権限・実行条件保持部が保持する権限内容の認証を行う請求項 1 に記載のエージェント連携システム（4）。

【 0 1 0 3 】

（付記 9）前記認証機構が、ポリシー管理機関と、属性管理機関と、個体認証管理機関の 3 つの機関に分かれ、

前記ポリシー管理機関が、ポリシーを記述したデータに対して電子署名を付し、真正のポリシーであることが認証されたポリシー証明書を発行し、

前記属性管理機関が、各エージェントが持っている属性を証明した属性証明書を発行し、

前記公開鍵管理機関が、ネットワーク上におけるエージェントの個体認証を行

った証明である公開鍵証明書を発行し、

各エージェントが、前記ポリシー証明書と属性証明書を解釈するトラストエンジンを備え、ネットワーク上で配布されたポリシー証明書と属性証明書に基づいて前記権限付与部に対して割り当てるべき適切な権限内容を指定する付記 8 に記載のエージェント連携システム（5）。

【 0 1 0 4 】

（付記 1 0）各エージェントが、前記仮想通信路への参加・不参加を自ら選択できる付記 1 に記載のエージェント連携システム。

【 0 1 0 5 】

（付記 1 1）各エージェントが、仮想通信路にログインする際に、前記トラストエンジンを用いて、当該仮想通信路に対応するポリシーの証明書と属性証明書を入力として、ポリシーの証明を得つつログインし、

各エージェントのログインの連鎖により仮想通信路に参加するエージェント間にポリシーを安全に伝播させることを特徴とする付記 9 に記載のエージェント連携システム（6）。

【 0 1 0 6 】

（付記 1 2）前記ポリシー記憶部が、相互独立のポリシーを複数生成・管理し、それらポリシーに従って情報をやり取りするエージェント間の連携を前記仮想通信路に相互独立に生成した付記 1 に記載のエージェント連携システム。

【 0 1 0 7 】

（付記 1 3）前記ポリシー記憶部が前記相互独立に生成・管理している複数のポリシーのうち選択されたポリシーを統合し、統合後のポリシーに従って情報をやり取りするエージェント間の連携を前記仮想通信路に生成する付記 1 に記載のエージェント連携システム。

【 0 1 0 8 】

（付記 1 4）前記ポリシー記憶部が、前記ポリシーを複数相互独立に分割し、分割後のポリシーごとに、それぞれのポリシーに応じて情報をやり取りするエージェント間の連携を前記仮想通信路に相互独立に生成する付記 1 に記載のエージェント連携システム。

【 0 1 0 9 】

(付記 1 5) 前記ポリシー記憶部は、第 1 のポリシーと、前記第 1 のポリシーに属し、前記第 1 のポリシーに対して新たなルールを追加した第 2 のポリシーを記憶し、前記第 1 のポリシーに応じたエージェント間の連携上に前記第 2 のポリシーに応じたエージェント間の連携を生成した付記 1 に記載のエージェント連携システム。

【 0 1 1 0 】

(付記 1 6) 他のエージェントに対して要求を出すエージェントは、要求情報の送信にあたり、前記ポリシーに従って要求情報に前記ラベル情報を付して送信し、

前記要求情報を受信し、前記要求に対する応答を実行した他のエージェントは、応答情報の送信にあたり、前記ポリシーに従って前記応答情報にラベル情報を付して送信し、

前記要求を出したエージェントは、前記ポリシーに従って前記ラベル情報を持つ応答情報を受信する付記 1 に記載のエージェント連携装置。

【 0 1 1 1 】

(付記 1 7) 前記権限保持部において保持されている権限が有効期限を持ち、有効期限の経過により該権限を無効化する付記 1 に記載のエージェント連携システム。

【 0 1 1 2 】

(付記 1 8) 前記ラベル情報が有効期限を持ち、有効期限の経過により各エージェントにおいて該ラベル情報の付されたメッセージを無視する付記 1 に記載のエージェント連携システム。

【 0 1 1 3 】

(付記 1 9) 前記仮想通信路が有効期限を持ち、有効期限の経過により該仮想通信路が消滅する付記 1 に記載のエージェント連携システム。

【 0 1 1 4 】

(付記 2 0) 前記仮想通信路上または前記エージェントに、前記仮想通信路に対する不正アクセスを検知する不正アクセス検知部を備え、

前記不正アクセス検知部により前記仮想通信路への不正アクセスを検知したことを契機として、各エージェントが前記仮想通信路への接続を断ち、前記仮想通信路を動的に消滅する付記 1 に記載のエージェント連携システム。

【 0 1 1 5 】

(付記 2 1) 前記仮想通信路上のいずれかのエージェントからの仮想通信路の消滅要求を受け、各エージェントが前記仮想通信路への接続を断ち、前記仮想通信路を動的に消滅させる付記 1 に記載のエージェント連携システム。

【 0 1 1 6 】

(付記 2 2) ネットワーク上に存在するエージェント間の情報通信を仲介する方法であって、前記仮想通信路上の各エージェントにおいて、

エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーを記憶し、前記ポリシーに従って各エージェントの属性に応じた権限を付与し、

前記付与された権限および該権限内容が実行される条件を保持・記憶し、

前記権限内容の実行条件が成立した場合に該当する権限内容を実行し、

前記ポリシーに従って前記仮想通信路を介して各エージェントを連携させることを特徴とするエージェント連携方法 (7)。

【 0 1 1 7 】

(付記 2 3) ネットワーク上に存在するエージェント間の情報通信を仲介する処理プログラムを記録したコンピュータ読み取り可能な記憶媒体であって、

エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーを記憶し、前記ポリシーに従って各エージェントの属性に応じた権限を付与する処理ステップと、

前記付与された権限および該権限内容が実行される条件を保持・記憶する処理ステップと、

前記権限内容の実行条件が成立した場合に該当する権限内容を実行する処理ステップと、

各エージェントが前記ポリシーに従って与えられた権限に応じてメッセージをやりとりするように前記仮想通信路を制御する処理ステップとを備えた処理プロ

グラムを記録したことを特徴とする記録媒体（８）。

【 0 1 1 8 】

（付記２４）ネットワーク上に存在するエージェント間の情報通信を仲介する通信路であって、

エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーに従って制御され、

前記ポリシーに従って各エージェントに対してその属性に応じた権限を持たせ

、  
前記ポリシーに従って動作するエージェント同士を仮想的に結び、前記権限内容の実行を通して各エージェントの連携処理を仲介することを特徴とする仮想通信路（９）。

【 0 1 1 9 】

【発明の効果】

本発明のエージェント連携システムおよびエージェント間を結ぶ仮想通信路によれば、エージェントの属性と該属性に対して割り当てられた権限との関係を表わすルールを含むルールの集合であるポリシーに従って制御され、ポリシーに従ってポリシーに従ってエージェント同士を仮想的に結び、エージェント間の連携を仲介できる。

【 0 1 2 0 】

本発明のエージェント連携システムは、ポリシーに基づいて、エージェント間の多様な連携形態を柔軟に構築・変更することができ、例えば、仮想通信路上に複数相互のエージェント間連携の構築、エージェント間連携の分割、統合、入れ子状態のエージェント間連携の構築などが可能である。

【 0 1 2 1 】

また、本発明のエージェント連携システムは、アクセス権管理、不正アクセス検知、メッセージの暗号化復号化処理を備えた構成とし、仮想通信路、エージェント間連携、メッセージ送受信に対するセキュリティを向上することができる。

【 0 1 2 2 】

また、本発明のエージェント連携システムは、ポリシーを一元的に管理し、頒

布するポリシーリポジトリサーバを備え、未だポリシーを持っていないエージェントに対するポリシーの頒布を実行でき、また、ポリシーそのものの更新がある場合においてエージェントに対して更新後のポリシーを頒布することができる。

【図面の簡単な説明】

【図 1】 本発明で用いるポリシー文法の一部の例を示した図

【図 2】 本発明の実施形態 1 のエージェント連携システムの装置構成例を模式的に示す図

【図 3】 本発明の実施形態 1 のエージェント連携システムにおける仮想通信路構築動作、エージェント連携動作例を示したフローチャート

【図 4】 (a) が複数相互のエージェント間連携の構築の様子を概念的に示したもの、(b) が複数相互のエージェント間連携を統合する様子概念的に示したもの、(c) がエージェント間連携を分割する様子概念的に示したもの、(d) がエージェント間連携の入れ子状態の様子を概念的に示したもの

【図 5】 本発明の実施形態 3 のポリシー証明とロール保証の概念を模式的に示す図

【図 6】 本発明の実施形態 3 のエージェント連携システムの装置構成例を模式的に示す図

【図 7】 本発明の実施形態 4 のエージェント連携システムの装置構成例を模式的に示す図

【図 8】 本実施形態 5 における本発明のオブジェクトエージェント連携システムを実現する処理プログラムを記録した記録媒体の例を示す図

【符号の説明】

5 ポリシー管理機関

6 属性管理機関

7 個体認証機関

8 トラストエンジン

10 エージェントネットワークコネクタ

11 アクセス権管理部

12 不正アクセス検知部

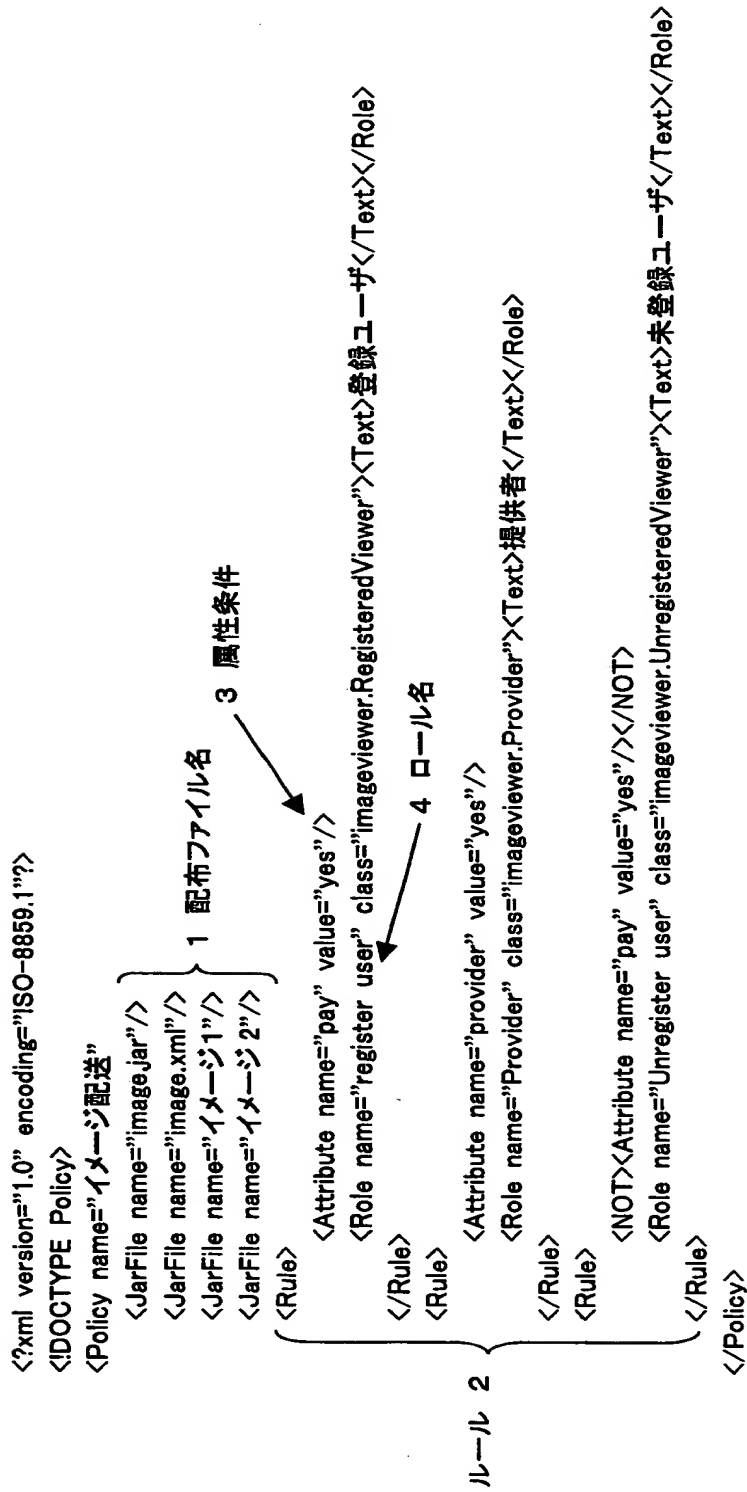
- 2 0 セキュリティマネージャ
- 3 0 ロールマネージャ
- 4 0 属性マネージャ
- 5 0 ロールプログラムデータベース
- 6 0 フィールドコネクタ
- 7 0 ロールメソッドテーブル
- 8 0 ロール実行部
- 9 0 エージェント連携確認部
- 1 0 0, 1 0 0 a エージェント
- 2 0 0 外部ネットワーク
- 2 1 0 内部フィールド
- 3 0 0 ポリシーリポジトリサーバ
- 1 0 0 0 記録装置内の記録媒体
- 1 0 0 1 可搬型記録媒体
- 1 0 0 2 C D - R O M
- 1 0 0 3 フレキシブルディスク
- 1 0 0 4 コンピュータ
- 1 0 0 5 コンピュータのハードディスクや R A M 等の記録媒体

【書類名】

図面

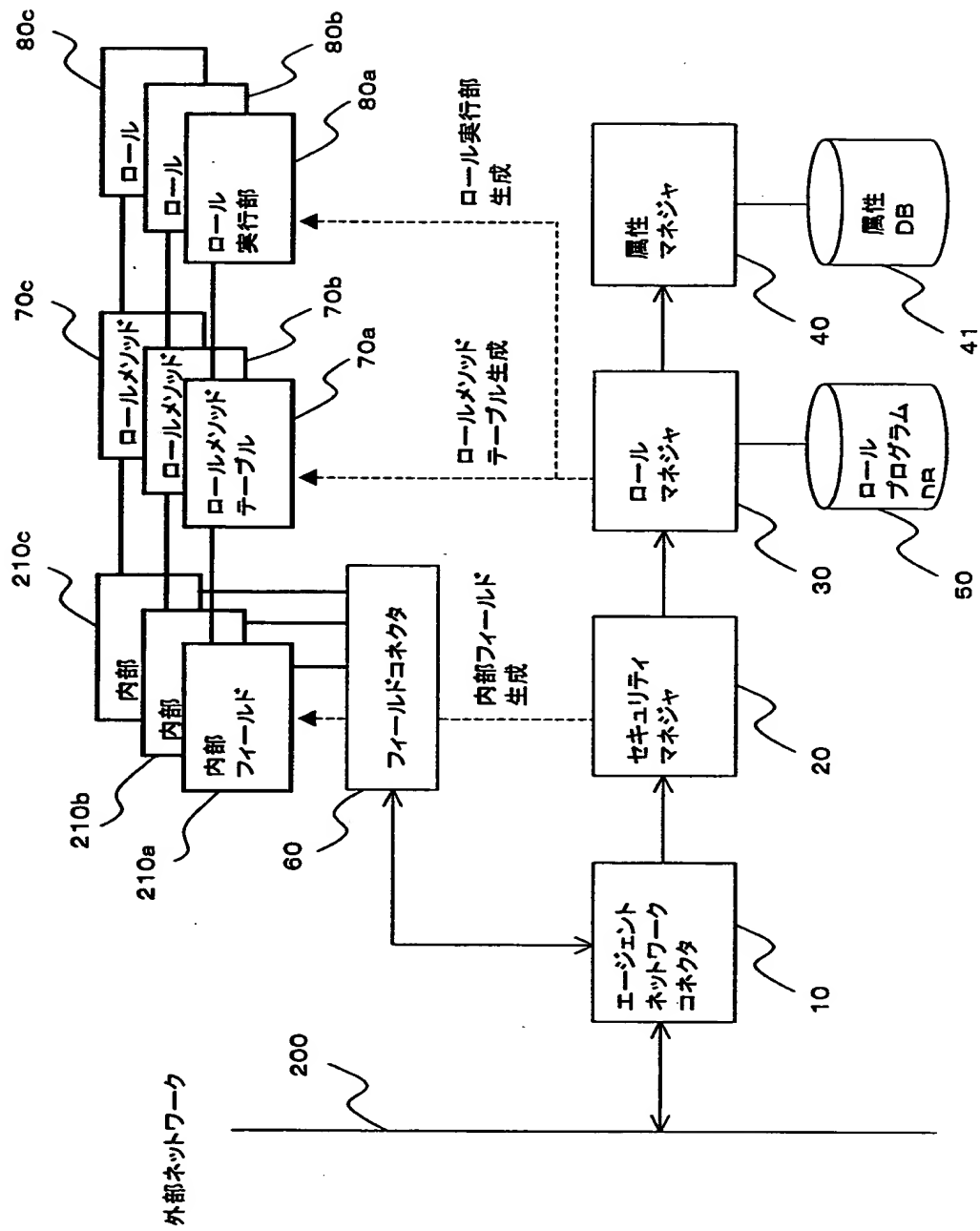
【図 1】

ポリシー記述例

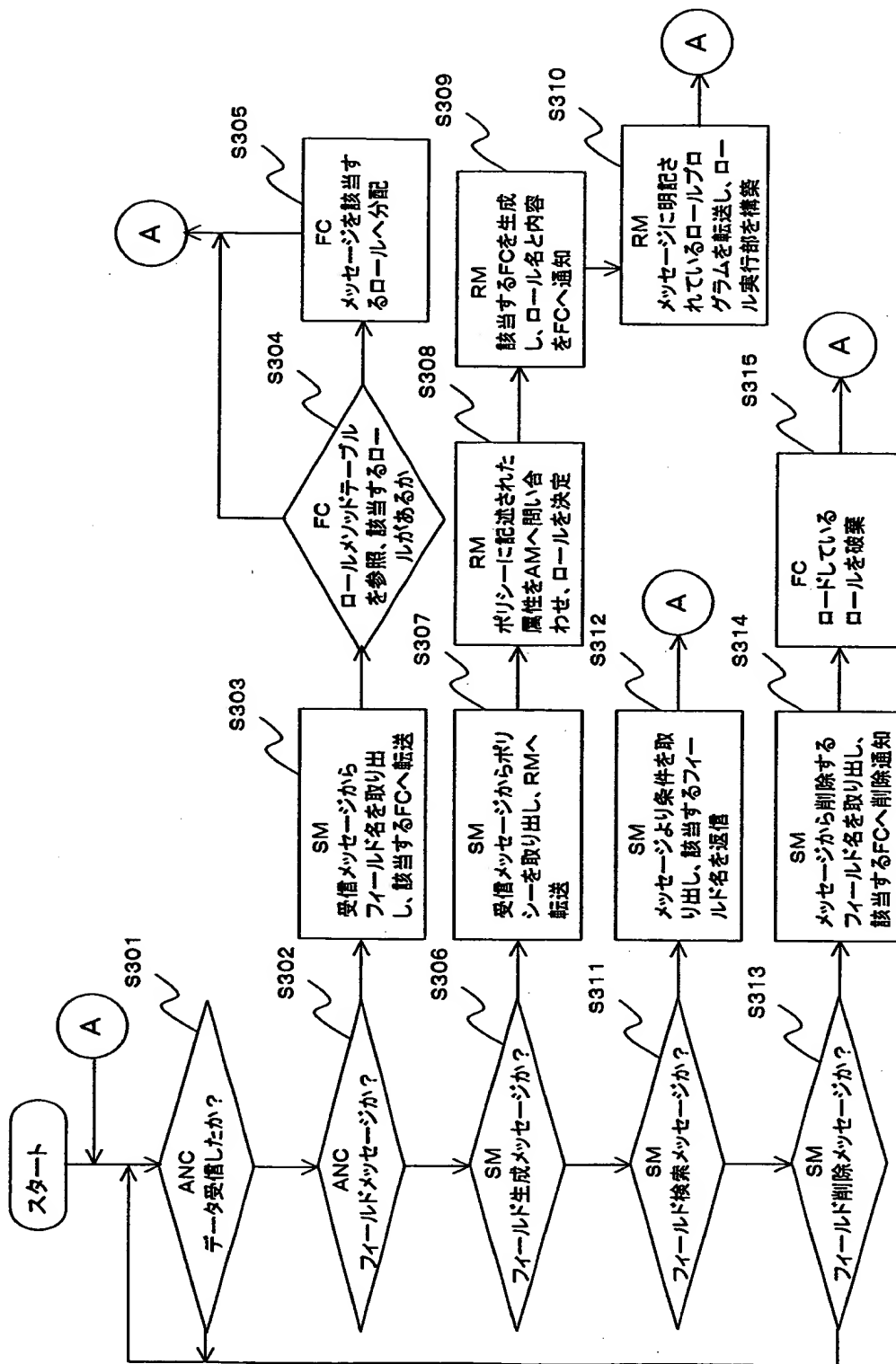




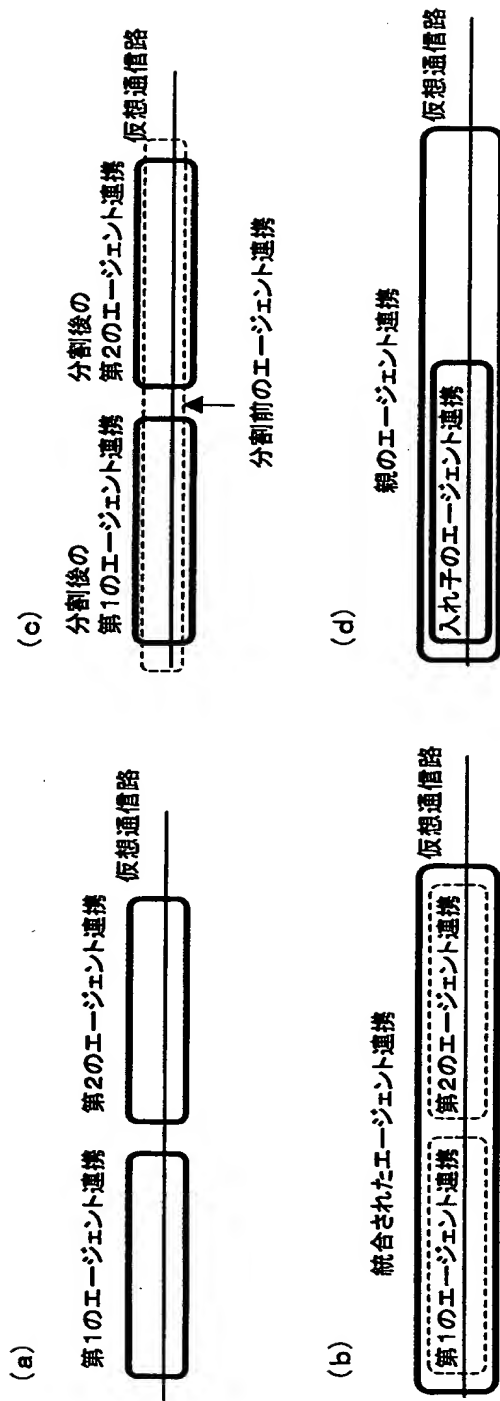
【図 2】



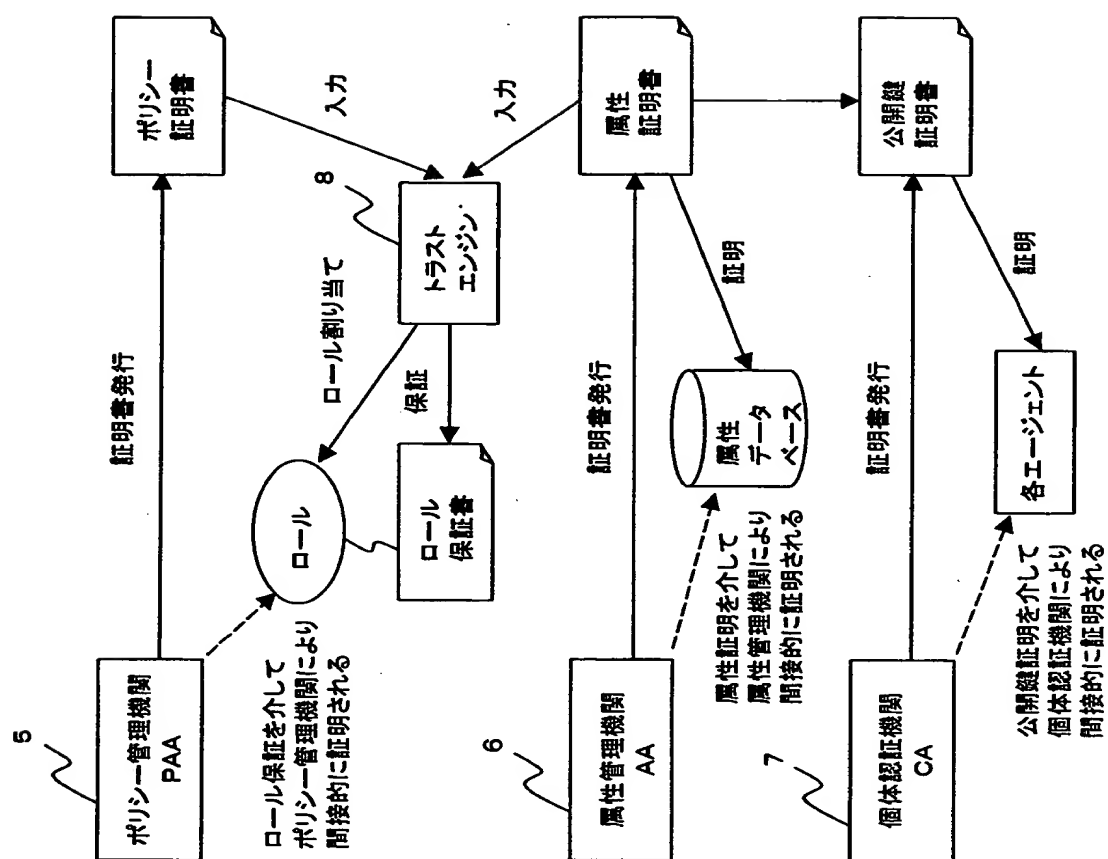
【図 3】



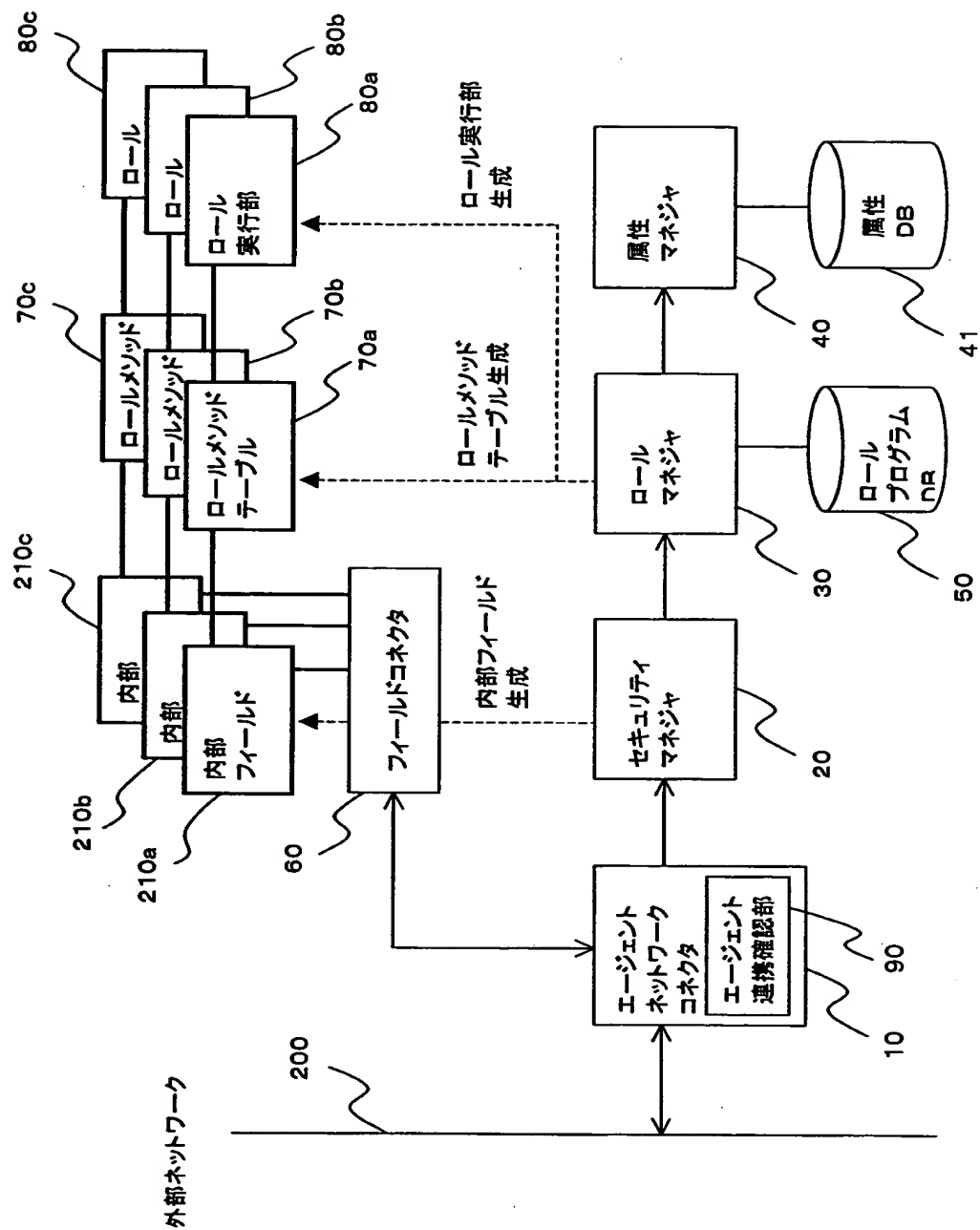
【図4】



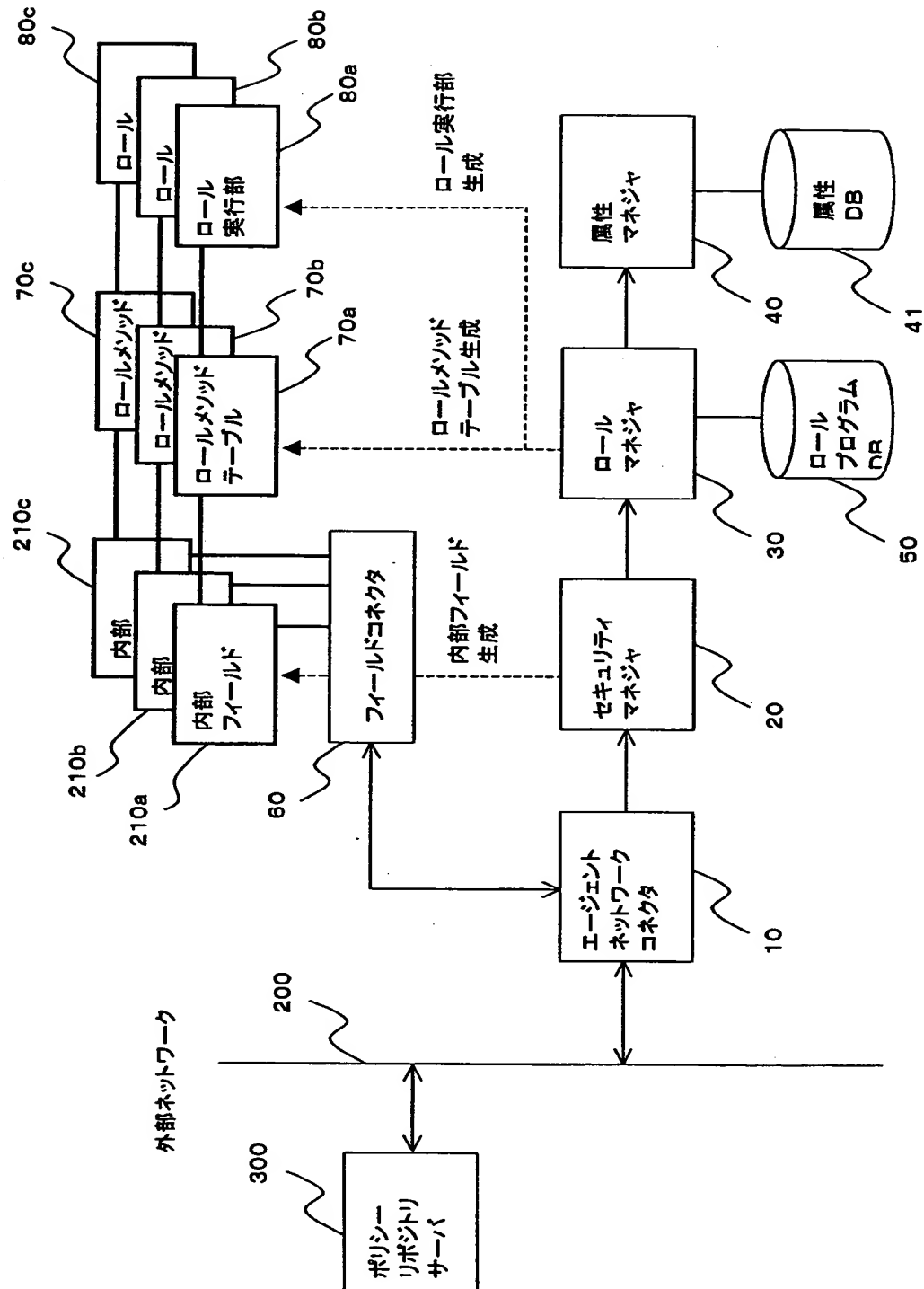
【図 5】



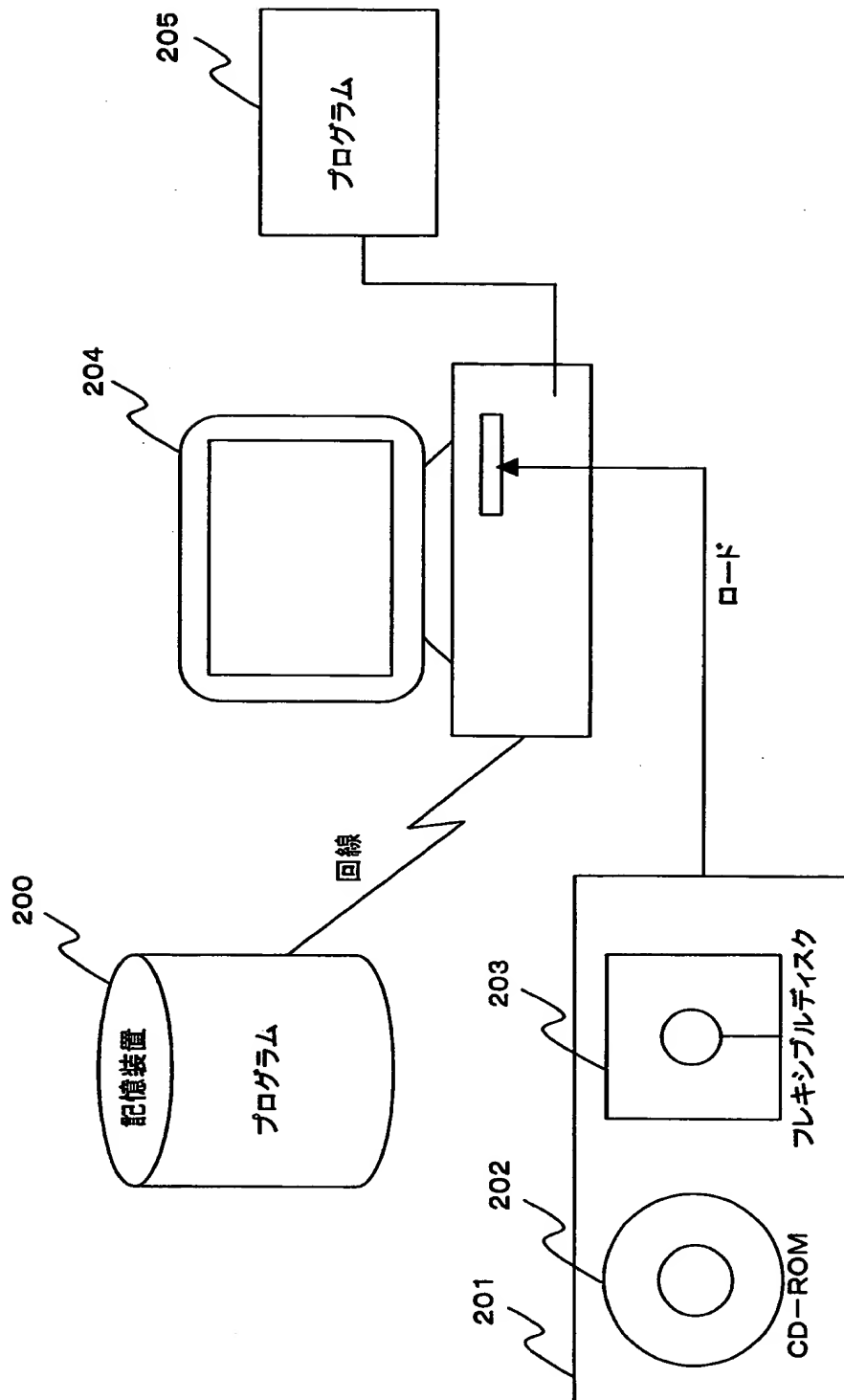
【図 6】



【図 7】



【図8】



【書類名】 要約書

【要約】

【課題】 要求やサービス内容に応じて情報を送受信する仮想通信路を柔軟かつ動的に構築し、エージェント間の連携を実現する。

【解決手段】 ネットワーク上の各エージェント 1 0 0 に対してエージェントの属性と権限を関係づけたポリシーを頒布する。セキュリティマネージャの指示によりフィールドコネクタ 6 0 が内部フィールド 2 1 0 を生成し、ロールマネージャ 3 0 は、属性マネージャからの属性情報を利用し、各エージェントの属性に応じた権限（ロール）を各エージェントに与え、ロールメソッドテーブル 7 0、ロール実行部 8 0 を構築する。各エージェントはメッセージを外部ネットワークから受け取るとロールメソッドテーブルを参照して該当するロールを検索し、ロール実行を行う。メッセージのやり取りを通じて仮想通信路を介したエージェント間の連携を実現する。

【選択図】 図 2



出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日	1996年 3月26日
[変更理由]	住所変更
住 所	神奈川県川崎市中原区上小田中4丁目1番1号
氏 名	富士通株式会社